WHAT IS CLAIMED IS:

1. A program distribution device for distributing executable programs through a network to a client device having a tamper resistant processor which is provided with a unique secret key and a unique public key corresponding to the unique secret key in advance, the program distribution device comprising:

a first communication path set up unit configured to set up a first communication path between the program distribution device and the client device;

a second communication path set up unit configured to set up a second communication path directly connecting the program distribution device and the tamper resistant processor, on the first communication path;

an encryption processing unit configured to produce an encrypted program by encrypting an executable program to be distributed to the client device; and

a transmission unit configured to transmit the encrypted program to the tamper resistant processor through the second communication path.

2. The program distribution device of claim 1, further comprising:

a user authentication unit configured to carry out authentication of a user who is using the client device, by using a user ID of the user received from the client device through the first communication path.

3. The program distribution device of claim 1, further comprising:

a processor authentication unit configured to carry out authentication of the tamper resistant processor, by verifying a certificate certifying that the tamper resistant processor surely has the unique secret key and

the unique public key, which is received from the client device through the second communication path.

4. The program distribution device of claim 1, wherein the encryption processing unit encrypts the executable program by using the unique public key received from the tamper resistant processor through the second communication path.

5. The program distribution device of claim 1, wherein the encryption processing unit encrypts the executable program by using a common key, and encrypts the common key by using the unique public key received from the tamper resistant processor through the second communication path; and

the transmission unit transmits the encrypted program along with an encrypted common key to the tamper resistant processor through the second communication path.

6. The program distribution device of claim 1, wherein communications through the second communication path are cipher communications.

7. A client device for receiving programs distributed from a program distribution device through a network, the client device comprising:

a tamper resistant processor which is provided with a unique secret key and a unique public key corresponding to the unique secret key in advance;

a first communication path set up unit configured to set up a first communication path between the program distribution device and the client device;

a second communication path set up unit configured to set up a second communication path directly connecting the program distribution device and the tamper resistant

processor, on the first communication path; and

a program receiving unit configured to receive an encrypted program from the program distribution device through the second communication path.

8. The client device of claim 7, further comprising:

a user authentication unit configured to carry out authentication of a user who is using the client device with respect to the program distribution device, by transmitting a user ID of the user to the program distribution device through the first communication path.

9. The client device of claim 7, further comprising:

a certification unit configured to carry out authentication of the tamper resistant processor with respect to the program distribution device, by transmitting a certificate certifying that the tamper resistant processor surely has the unique secret key and the unique public key, through the second communication path.

10. The client device of claim 7, wherein the program receiving unit receives the encrypted program which is encrypted by using the unique public key notified from the tamper resistant processor to the program distribution device through the second communication path.

11. The client device of claim 7, wherein the program receiving unit receives the encrypted program which is encrypted by using a common key, and an encrypted common key which is encrypted by using the unique public key notified from the tamper resistant processor to the program distribution device through the second communication path.

12. The client device of claim 7, wherein communications through the second communication path are cipher

communications.

13. A program distribution system, comprising:

a program distribution device connected to a network, for distributing executable programs through the network; and

a client device connected to the network, for receiving the executable programs distributed from the program distribution device through the network;

wherein the client device has:

a tamper resistant processor which is provided with a unique secret key and a unique public key corresponding to the unique secret key in advance;

a client side first communication path set up unit configured to set up a first communication path between the program distribution device and the client device;

a client side second communication path set up unit configured to set up a second communication path directly connecting the program distribution device and the tamper resistant processor, on the first communication path; and

a program receiving unit configured to receive an encrypted program from the program distribution device through the second communication path;

and the program distribution device has:

a server side first communication path set up unit configured to set up the first communication path between the program distribution device and the client device;

a server side second communication path set up unit configured to set up the second communication path directly connecting the program distribution device and the tamper resistant processor, on the first communication path;

an encryption processing unit configured to produce the encrypted program by encrypting an executable program to be distributed to the client device; and

a transmission unit configured to transmit the

encrypted program to the tamper resistant processor through the second communication path.

14. A method for distributing executable programs through a network from a program distribution device to a client device having a tamper resistant processor which is provided with a unique secret key and a unique public key corresponding to the unique secret key in advance, the method comprising the steps of:

setting up a first communication path between the program distribution device and the client device;

setting up a second communication path directly connecting the program distribution device and the tamper resistant processor, on the first communication path;

producing an encrypted program by encrypting an executable program to be distributed to the client device, at the program distribution device; and

transmitting the encrypted program from the program distribution device to the tamper resistant processor through the second communication path.

15. The method of claim 14, further comprising the step of:

carrying out authentication of a user who is using the client device, by using a user ID of the user received from the client device through the first communication path.

16. The method of claim 14, further comprising the step of:

carrying out authentication of the tamper resistant processor, by verifying a certificate certifying that the tamper resistant processor surely has the unique secret key and the unique public key, which is received from the client device through the second communication path.

17. The method of claim 14, wherein the producing step encrypts the executable program by using the unique public key received from the tamper resistant processor through the second communication path.

18. The program distribution device of claim 1, wherein the producing step encrypts the executable program by using a common key, and encrypts the common key by using the unique public key received from the tamper resistant processor through the second communication path; and

the transmitting step transmits the encrypted program along with an encrypted common key to the tamper resistant processor through the second communication path.

19. The method of claim 14, wherein communications through the second communication path are cipher communications.